

**Citycom's Response to the TRAI Consultation Paper on Net Neutrality;
dated 4th January 2017**

Q1. What could be the principles for ensuring nondiscriminatory access to content on the Internet, in the Indian context? [See Chapter 4]

Comments:

We are of the view that current legitimate traffic management practices should continue subject to the core principles listed below.

- Adequate disclosure to users about traffic management policies and tools to allow them to make informed choices.
- Application-agnostic controls may be used but application-specific control within the Internet traffic" class may not be permitted.

Q2. How should "Internet traffic" and providers of "Internet services" be understood in the NN context? [See Chapter 3]

(a) Should certain types of specialised services, enterprise solutions, Internet of Things, etc be excluded from its scope? How should such terms be defined?

(b) How should services provided by content delivery networks and direct interconnection arrangements be treated?

Please provide reasons.

Comments:

A publicly available electronic service that provides access to the Internet, and thereby connectivity to virtually all end points of the Internet, irrespective of the technology or the terminal equipment used.

Our definition of Internet Services would be any service that provides generic connectivity to all Internet public IPs.

We are of the view that it would be prudent to exclude some services from the NN purview.

Enterprise Solutions: Enterprise solutions are very dependent on guaranteed QoS towards certain services and servers. Hence it might be prudent to exclude enterprise solutions from NN purview.

IOT: In our view, a vast majority of IOT services will be generic and should come under NN purview. Exception might be provided for only IOT for Emergency Services which will require guaranteed QoS.

It is our view that content from CDN networks and direct interconnection arrangements be treated as Network optimization solutions, this will improve the QoS to the customer.

Network optimization solutions such as interconnection arrangements, caching or content delivery network (CDN) services that offer a benefit by reducing the total distance of travel, not only improve the quality of service for those using the solution but also for other users that share the same local network of the ISP/TSP. This is because such solutions decongest the existing access network. Therefore, offering a benefit of improved performance through network optimization solutions (such as faster interconnection, caching or CDN services), rather improves their experience. In this context, improving overall performance through network optimization should be welcome.

Hence, provisioning of services by network optimization solutions by establishing CDN networks and direct interconnection agreements are in the right direction since it enhances the end user experience. These should be allowed and no restrictions should be applied for these.

Q3. In the Indian context, which of the following regulatory approaches would be preferable: [See Chapter 3]

- (a) Defining what constitutes reasonable TMPs (the broad approach), or**
- (b) Identifying a negative list of non-reasonable TMPs (the narrow approach).**

Please provide reasons.

Comments:

It would be good to have the narrow approach regulations of explicitly stating what is not acceptable. This would allow the ISPs/TSPs to frame their own policies for network optimization and market innovation.

Q4. If a broad regulatory approach, as suggested in Q3, is to be followed: [See Chapter 3]

- (a) What should be regarded as reasonable TMPs and how should different categories of traffic be objectively defined from a technical point of view for this purpose?**
- (b) Should application-specific discrimination within a category of traffic be viewed more strictly than discrimination between categories?**
- (c) How should preferential treatment of particular content, activated by a user choice, and without any arrangement between a TSP and content provider, be treated?**

Comments:

It is our view, as indicated in Q.3 that a narrow approach should be followed for TMP.

Yes, application-specific discrimination within a category of traffic should be viewed more strictly than discrimination between categories

We are of the view that preferential treatment of any particular content should not be allowed.

Q5. If a narrow approach, as suggested in Q3, is to be followed what should be regarded as non reasonable TMPs? [See Chapter 3]

Comments:

The following may be considered as non-reasonable Traffic Management Practice:

- (i) Providing differential QoS toward a certain CDN, IP Pool for internet traffic.
- (ii) Giving preferential QoS to specific applications
- (iii) After application identification giving preferential QoS to an application of Vendor A and retarded QoS to an application from Vendor B.

Q6. Should the following be treated as exceptions to any regulation on TMPs? [See Chapter3]

- (a) Emergency situations and services;**
- (b) Restrictions on unlawful content;**
- (c) Maintaining security and integrity of the network;**

- (d) Services that may be notified in public interest by the Government/ Authority, based on certain criteria; or**
- (e) Any other services.**

Please elaborate.

Comments:

- (a) Emergency situations and services
Yes, but these exceptions need to be clearly defined and unambiguous.
- (b) Restrictions on unlawful content
Yes, as per prevalent laws and constitutional rights.
- (c) Maintaining security and integrity of the network
Yes, narrowly tailored on a nondiscriminatory non-interference basis for a limited time in the area or portion of network effected.
- (d) Services that may be notified in public interest by the Government/ Authority, based on certain criteria
Yes. Here again the services will have to be narrowly tailored and criteria be made specific. The public interest be specified and be publicly announced. The notified public interest should stand the test of freedom of speech and constitutional rights.

Q7. How should the following practices be defined and what are the tests, thresholds and technical tools that can be adopted to detect their deployment: [See Chapter 4]

- (a) Blocking;**
- (b) Throttling (for example, how can it be established that a particular application is being throttled?); and**
- (c) Preferential treatment (for example, how can it be established that preferential treatment is being provided to a particular application?).**

Comments:

- (a) Blocking

Blocking is currently being done based on directives that the ISP/TSP's receive from the DOT/ Licensor, competent court order and Law Enforcement Agencies. Apart from the above requirements TSPs/ISPs should not carry out any blocking themselves.

- (b) Throttling (for example, how can it be established that a particular application is being throttled?)

We are of the view that throttling of a particular application will be hard to detect unless there are test devices which are available in neutral network beyond the TSP network wherein these test devices can, in tandem with user clients, do a performance/throughput test between point A and B across various applications. As long as the IP throughput regardless of the application is the same, there is no throttling. This needs to take into account things like packet rate and frame size etc.

The licensor/regulator should appoint an independent neutral agency to carry out this testing.

- (c) Preferential treatment (for example, how can it be established that preferential treatment is being provided to a particular application?)

The licensor/regulator should appoint an independent neutral agency to carry out this testing.

In principle, Preferential treatment is almost similar to what has been stated in point 7(b) above where one looks for applications with higher performance/throughput compared to others.

Q8. Which of the following models of transparency would be preferred in the Indian context: [See Chapter 5]

- (a) Disclosures provided directly by a TSP to its consumers;**
- (b) Disclosures to the regulator;**
- (c) Disclosures to the general public; or**
- (d) A combination of the above.**

Please provide reasons. What should be the mode, trigger and frequency to publish such information?

Comments:

In our view a combination of 'a' and 'b' would be preferable in the Indian context. Disclosure to the general public might not be necessary as the disclosure sought here are more technical in nature and it may not be

necessary for a TSP to disclose its TMP etc., if any to general public at large who is not its subscriber per se.

We are of the view that positive assurance by way of declaration or disclosures by TSPs to Authority/Regulator shall be made mandatory. Disclosure to a subscriber shall be provided upon specific request being made by the Subscriber in writing. While considering the above, we would also request the Authority to take into consideration the provision of safeguards for trade secrets and information that might give a competitive advantage to a TSP over another.

Q9. Please provide comments or suggestions on the Information Disclosure Template at Table 5.1? Should this vary for each category of stakeholders identified above? Please provide reasons for any suggested changes. [See Chapter 5]

Comments:

The information disclosure template is exhaustive and covers all aspects well. In our view it would be difficult to mention typical latency and packet loss unless a standard endpoint is defined.

In our view the template is good for the regulator and some aspect can be shared with customers on request. Items like application specific/agnostic data should be shared only with the regulator as this information might be used for competitive advantage or generating application specific DDOS attacks.

Q10. What would be the most effective legal/policy instrument for implementing a NN framework in India? [See Chapter 6]

- (a) Which body should be responsible for monitoring and supervision?**
- (b) What actions should such body be empowered to take in case of any detected violation?**
- (c) If the Authority opts for QoS regulation on this subject, what should be the scope of such regulations?**

Comments:

Existing framework of licensing authority and TRAI are adequate. For monitoring and supervision a multilateral empowered agency should be created having representatives of Licensor, TRAI and Industry experts.

If the Authority opts for QoS Regulation on this subject, the scope should be as per the standard practices followed by TRAI on QoS of other services.

Q11. What could be the challenges in monitoring for violations of any NN framework? Please comment on the following or any other suggested mechanisms that may be used for such monitoring: [See Chapter 6]

- (a) Disclosures and information from TSPs;**
- (b) Collection of information from users (complaints, user-experience apps, surveys, questionnaires); or**
- (c) Collection of information from third parties and public domain (research studies, news articles, consumer advocacy reports).**

Comments:

As we recommended in Q. 10(a) that an empowered and competent agency should be set up to investigate and monitor net neutrality by service providers. This agency should evolve its own best practices based on experience.

In our view the same empowered multilateral agency suggested above should monitor disclosures and information from TSPs and use this information to verify by testing.

At this stage the net neutrality understanding by users is at a nascent stage and hence information from users may not be depended upon. The empowered agency should evolve its own best practices.

Q12. Can we consider adopting a collaborative mechanism, with representation from TSPs, content providers, consumer groups and other stakeholders, for managing the operational aspects of any NN framework? [See Chapter 6]

- (a) What should be its design and functions?**
- (b) What role should the Authority play in its functioning?**

Comments:

The primary functions should be to check for violations of net neutrality as defined by the Authority.

The empowered agency we have suggested in response to Q10 should function under the broad umbrella of the Authority.

Q13. What mechanisms could be deployed so that the NN policy/regulatory framework may be updated on account of evolution of technology and use cases? [See Chapter 6]

Comments:

The empowered agency would have experts and hence be competent to evaluate newer and evolving technologies and applications. Regulations should also evolve in tandem with evolving technologies.

Q14. The quality of Internet experienced by a user may also be impacted by factors such as the type of device, browser, operating system being used. How should these aspects be considered in the NN context? Please explain with reasons. [See Chapter 4]

Comments:

The user experience based on end device, browser, OS, processing power should be outside the purview of NN. The network, TSPs or the content provider would not be able to influence this in anyway.

* * * * *